Survey On Intrusion Detection System

Prof.A.K.Gulve
Dept of CSE, G.E.C,Aurangabad
akgulve@yahoo.com

D.G.Vyawahare
ME(Final Year), GEC,Aurangabad
dgvyawahare@acm.org

ABSTRACT

This paper presents a survey of two techniques of intrusion detection system using supervised and unsupervised learning. The techniques are categorized based upon different approaches like Statistics, Data mining, Neural Network Based and Self Organising Maps Based approaches. The detection type is borrowed from intrusion detection as either misuse detection or anomaly detection. It provides the reader with the major advancement in the malware research using these approaches the features and categories in the surveyed work based upon the above stated categories. This served as the major contribution of this paper.

1 INTRODUCTION

Computer networks and systems have become indispensable tools for modern business. Much of this information is, to some degree, confidential and its protection is required. Not surprisingly then, intrusion detection systems (IDS) have been developed to help uncover attempts by unauthorized persons and/or devices to gain access to computer networks and the information stored therein. In addition, network devices such as routers and firewalls maintain activity logs that can be used to examine such attempts.

Intrusion detection may be regarded as the art of detecting inappropriate, incorrect or anomalous activity within or concerning a computer network or system. The most common approaches to intrusion detection are statistical anomaly detection and pattern-matching detection. IDS that operate on a host to detect malicious activity on that host are called host-based IDS (HIDS), which may exist in the form of host wrappers/personal firewalls or agent-based software, and those that operate on network data flows are called network-based IDS (NIDS). Host-based intrusion detection involves loading software on the system (the host) to be monitored and using log files and/or the host's auditing agents as sources of data. In contrast, a network-based intrusion detection system monitors the traffic on its network segment and uses that traffic as a data source. Packets captured by the network interface cards are considered to be of interest if they match a signature.there are basically four types of approaches as follows.

1.1 Statistics-Based Approaches:

According to audit data, a profile is constructed to describe a given subject (network user) or a given object (task). Several metrics are defined for the profiles. The Gaussian models of the metrics are constructed to detect intrusions.

1.2 Data-Mining-Based Approaches:

Data mining is used in intrusion detection to construct rules describing normal network behaviors. The rules include association rules that describe frequency associations between any two fields of the network record database and also frequent episodes that describe the frequency with which a field takes a certain value after two other fields have particular values in a definite time interval. Deviations from these rules indicate an attack on the network.

1.3 Supervised Learning-Based Approaches:

Recently, methods from machine learning and pattern recognition have been utilized to detect intrusions. Supervised learning and unsupervised learning are both used. For supervised learning for intrusion detection, there are mainly supervised neural network (NN)-based approaches & support vector machine (SVM)-based approaches

1.4 Unsupervised Learning-Based Approaches:

Supervised learning methods for intrusion detection can only detect known intrusions. Unsupervised learning methods can detect the intrusions that have not been previously learned. Examples of unsupervised learning for intrusion detection include *K*-means-based approaches and self-organizing feature map (SOM).

SOM-based approaches: Some authors used the extract features that describe network behaviors from audit data, and they use the SOM to detect intrusions. Kayacik *et al.* propose a hierarchical SOM approach for intrusion detection. Specific attention is given to the hierarchical development of abstractions, which is sufficient to permit direct

labeling of SOM nodes with connection type. In a hierarchical SOM for intrusion detection used the classification capability of the SOM on selected dimensions of the data set to detect anomalies.

Their results are among the best known for intrusion detection.

Current approaches for intrusion detection have the following two problems.

a) Current approaches often suffer from relatively high false-alarmrates, whereas they have high detection rates. As most network behaviors are normal, resources are wasted on checking a large number of alarms that turn out to be false.

b) Their computational complexities are oppressively high. This limits the practical applications of these approaches.

2 RELATED WORK

2.1 Supervised Learning :

A. H. M. Rezaul Karim et al. (2006) proposed a collaborative IDS for MANET using Bayesian method using a set of very useful features which guarantee the effectiveness of the IDS. The Bayesian method improves the efficiency in the detection procedure.

They used the popular network simulator tool NS2 (ns-2.29) to measure the performance of the proposed IDS for mobile ad hoc network. the simulation parameters used were Sending capacity = 2Mps, Total number of flows = 42, Average transmission rate = 512 byte/packet, Packet type = TCP, Routing protocol = AODV, Training period = 1000s, Testing period = 30s

At the first step of simulation, they simulate a mobile ad hoc network using 50 nodes and other parameters for 1000 seconds. Six different attacks were simulated. They were Packet, Malicious, Rushing, Sleep deprivation, Routing table, Overflow and Routing table poisoning type attacks.

The effectiveness of the proposed IDS was evaluated using the performance measurement by the following parameters. True Positives (TP): The number of malicious nodes correctly classified as malicious. True Negatives (TN): The number of gentle nodes correctly classified as gentle. For earlier mentioned six attacks the IDS experienced 94.54% overall detection rate. It was highest i.e. 95.83% for Routing table type attacks.

L. Khan and et al (2007) proposed a method with a scalable solution for detecting network based anomalies. They used Support Vector Machines (SVM) for classification.. Thus investigating for enhancing the training time of SVM, specifically when dealing with large data sets, using hierarchical clustering analysis.

They used the Dynamically Growing Self-Organizing Tree (DGSOT) algorithm for clustering. A new approach of combination of SVM and DGSOT was made, which starts with an initial training set and expands it gradually using the clustering structure produced by the DGSOT algorithm. The approach was compared with the Rocchio Bundling technique and random selection in terms of accuracy loss and training time gain using a single benchmark real data set.

Accuracy rate of this SVM + DGSOT is the best for DOS type of attack, which is 97% and it is better as compared to pure SVM.. FN is lowest (3% for DOS) for SVM + DGSOT and FP rate is as low as pure SVM (2%). Whereas for U2R type of attacks the performance is poor. In this case the accuracy is found only 23% with FP 100% and FN 76%.

Tsong and et al.(2007) introduced a three-tier architecture of intrusion detection system which consists of a blacklist, a whitelist and a multi-class support vector machine classifier.They designed a three-tier IDS based on the KDD'99 benchmark dataset.

Their approach is based on the ensemble of blacklist/whitelist, thus to build a blacklist at the first tier and a whitelist at the second tier. Then they used one against one multiclass SSVMs [4] classification method at the third tier to classify those anomalies detected by whitelist into the four attack categories. This design was supposed to take the merits of MD and AD for intrusion detection purpose. The last tier, SVM classifier, categorize the attack into four classes: PROBE, DoS,R2L and U2R. The detection performance of this three-tier IDS was found up to 94.71% and the false alarm rate was only 3.8%. They concluded that their results are better than those of KDD'99 winner's.

Weiming Hu and et.al (2008) proposed an intrusion detection algorithm based on the AdaBoost algorithm. The discrete AdaBoost algorithm was selected to learn the classifier. In their algorithm, they selected decision stumps as weak classifiers. A decision stump is a decision tree with a root node and two leaf nodes. For each feature in the input data, a decision stump were constructed for detecting intrusions regarding basic features of individual Transmission Control Protocol (TCP) connections, content features within a connection suggested by domain knowledge, and traffic features computed By using this algorithm False alarm rate ranges from 0.31-1.79% with detection rate 90.04%-90.88% as compared to Genetic Clustering method giving 0.3% false alarm rate with detection rate as 79%. and RSS-DSS method giving 0.27%-3.5% false alarm rate with detection rate varying from 89.2% to 94.4%.

Hu Zhengbing1 and et al,(2008) proposed an algorithm to use the known signature to find the signature of the related attack quickly. They used nine different-sized databases, From 10Mbytes to 90Mbytes. They apply the Scan- Reduction method for reducing scanning times of database. By these approaches, they could find out the new attacking signature more efficiently than the Signature Apriori algorithm. For minimum support rate between 0.6 to 0.9 the processing time with scan reduction method is found to be 50 sec but for without scan reduction method it was 100 sec. The results were obtained for database size of 10 Mb.

Amit Kumar Choudhary and et al (2009) proposed a neural network approach to improve the alert throughput of a network and making it attack prohibitive using IDS. For evolving and testing intrusion the KDD CUP 99 dataset were used.

They proposed the Generalized Regression Neural Network (GRNN) paradigm as an alternative to the popular backpropagation training algorithm for feedforward neural networks. . The promising results of the present study shown the potential applicability of ANNs for developing high efficiency practical IDSs.

This Neural Network model solved normal attack attack patterns, and the type of the attack. When given data was presented to the model, the results obtained revealed a great deal of accuracy app. 100%.

2.2 Unsupervised Learning:

Giovanni Vigna and et al. (2003) developed a framework, called STAT, that supports the development of new intrusion detection functionality in a modular fashion. The STAT framework can be extended following a well-defined process to implement intrusion detection systems tailored to specific environments, platforms, and event streams.. The resulting intrusion detection systems represent a software family whose members share common attack modeling features and the ability to reconfigure their behavior dynamically. To be more precise, they developed an application, called *xSTAT*, that acts as a generic wrapper around the STAT runtime.

They proposed that developing a family of systems using an object-oriented framework reduces the development time and allows one to build compete intrusion detection system in a small amount of time. The STAT Framework is an approach for the development of intrusion detection systems based on the State Transition Analysis Technique..

They evaluated the performance impact of the framework based approach by comparing the performance of the original, *ad hoc* version of NetSTAT to the one developed by extending the STAT framework. The two systems were ran on a file containing two days worth of network data from the 1999 MIT Lincoln Laboratory evaluation. The total CPU time was collected for both sensors during multiple runs. The average processing time was 3,220 seconds for the original NetSTAT and 2,862 seconds for the framework based sensor. The speedup of 13.8% is attributed to careful optimization of the framework source code.

Stefano Zanero and et al. (2004) proposed a novel architecture which implements a network-based anomaly detection system using unsupervised learning algorithms. They described how the pattern recognition features of a Self Organizing Map algorithm can be used for Intrusion Detection purposes on the payload of TCP network packets.

They used a two-tier architecture, which allows us to retain at least part of the information related to the payload content. Their final goal was to detect intrusions, separate packets with anomalous or malformed payload from normal packets

The prototype was ran over various days of the 1999 DARPA dataset. A 66.7% detection rate with as few as 0.03% false positives was obtained. The detection rate was maximum upto 88.9% for threshold 0.09% with a false positive rate 0.095%.

Liberios VOKOROKOS (2006) presented intrusion detections systems and design architecture of intrusion detection based on neural network self organizing map. Result of the designed architecture is simulation in real conditions.

The goal of the proposed architecture was to investigate effectiveness of application of a neural network at modeling user behavioral patterns so that they can distinguish between normal and abnormal behavior. Expected network reply was the value closeto-for user, which behavior not diverting from normal behavior. If the output value of network becomes above specified threshold value, alarm was raised.

The results were obtained on the department server KPI Technical university of Košice. neural network SOM in the IDS systems. Collecting of essential information from single controlled points lasts 2 days. Next the neural network SOM was created and trained, which serves as the core of the IDS system. The results shown that input vectors classification, which represents behavior and its mapping to particular neurons, form single possible user behavior states. Formed states were as intrusion – Intrusion, possible intrusion – Intrusion?,

H. Günes Kayacık and et al.(2006) focused on developing behavioral models of known attacks to help security experts to identify the similarities between attacks. A Self Organizing Feature Map (SOM) was employed to model the relationship between known attacks and UMatrix representation was used to create a two dimensional topological map of known attacks. The approach was evaluated on KDD'99 data set. Results showed that attacks with similar behavior patterns are placed together on the map.

Considering the dataset needs to be balanced to eliminate any bias towards majority classes, they trained a Self-Organizing Map on the balanced training data and employed the labels (i.e. attack types) from the same dataset to assign labels to neurons. The concept of a best matching node was used to facilitate the labeling of the map.

Results on the test data indicate that known attacks are identified with relatively high identification accuracy although SOM employs unsupervised learning.

By using KDD 10 % dataset accuracy of attacks like perl, smurf, back, nmap found to be 100%,99.99%,88.24% and 48.48% respectively and that with corrected dataset accuracy of attacks like perl reduced to 50%, whereas back & nmap increased to 100%.

Zhenwei YU and et al. (2008), They presented an automatically tuning intrusion detection system, which controls the number of alarms output to the system operator and tunes the detection model on the fly according to feedback provided by the system operator when false predictions are identified. The system was evaluated using the KDDCup'99 intrusion detection dataset.

They proposed an adaptive and automatically tuning intrusion detection system, ADAT: Here, a prediction filter is used to push only the most suspicious predictions to the system operator to be verified. The volume of predictions is adjusted corresponding to the operator's ability to respond to predictions to be verified in order to avoid overwhelming the system operator. Second, the system tunes the detection model when false predictions are identified and adjusts the tuning strength based on monitoring the performance of the detection model on earlier data.

The results shown demonstrated that the ADAT model tuner improved the overall classification accuracy while decreasing total misclassification cost. Compared to the multiclassifier SLIPPER-based IDS without the tuning feature, ADAT reduced total misclassification cost (52294 as compared to 70177 of MC-Slipper) by 25.5%, while increasing overall accuracy by 1.78%. Compared to the automatically tuning IDS with delayed tuning, ADAT reduced TMC by 6.76%.

Stefano Zanero (2008) , presented a tool for network anomaly detection and network intelligence which was named as ULISSE. It uses a two tier architecture with unsupervised learning algorithms to perform network intrusion and anomaly detection. ULISSE uses a combination of clustering of packet payloads and correlation of anomalies in the packet stream.

In order to evaluate the architecture in a repeatable manner, the prototype was ran over various days of tra_c drawn from the 4th week of the 1999 DARPA dataset [14]. They also added various attacks against the Apache web server and against the Samba service generated through the Metasploit framework (www.metasploit.org).

It was concluded that their architecture can reach the same detection rate of 66.7% (PAYL [15]) with a false positive rate below 0.03%, thus an order of magnitude better than PAYL, or on the other hand reach a 88.9% detection rate with no more than a 1% rate of false positives.

V. K. Pachghare and et al.(2009) developed their own packet sniffer. Apart from capturing live packetsthey also used a standard DARPA dataset, for training purpose [17]. The dataset contain both packets with intrusion and without intrusion. The accepted window length was 20 for the application. Since the data were collected in every 20 seconds an input vector correspond to time interval of 400 seconds.

For training purpose they constructed a 30x30 Self Organizing Map in order to perform clustering. The data that was used for it was DARPA dataset [17]. Batch training algorithm with training

length 100 and starting radius 15 was used. Self organizing map was found largely successful in classifying the IP packets.

After the data collection, vector extraction and training of the Self Organizing Maps, the packets were passed through the SOM. The result were shown in form of patterns.

They concluded that, the actual experiments show that even a simple map, when trained on normal data, can detect the anomalous features of both buffer overflow intrusions exposed to it. This approach found particularly powerful because the self organizing map never needs to be told what intrusive behavior looks like [18].

Mansour M. Alsulaiman and et al. (2009) They built an Intrusion Detection System using a well known unsupervised neural network, namely Kohonen maps. They proposed two enhancements that were able to solve one of the shortcomings of the available solutions, namely high value of false positive rate. The method called as Performance-Based Ranking Method [21] was used. It works by deleting an input from the dataset and comparing the result before and after the deletion. They used the KDD data set which is available in [20].

To make the data in the right format, as an input to their system, they changed some of its feature formats, because neural network accept only numeric data. They changed 3 features, namely the protocol, flag and service to numeric data.

After this they tried to find ways to improve the results by proposing and investigating several enhancements to HSOM. HSOM was a powerful improvement to SOM, so they used it and got some good results. Thus they found ways to improve it. One enhancement was to complement it with PBRM and good results were obtained. Another enhancement was to add more layers. They showed that by good analysis and selecting the best layer to compliment a combination better results can be obtained.

The two enhancements were presented :

A. HSOM With PBRM : They applied the unresolved patterns of Net3 to a trained PBRM network, The PBMR classified the unresolved patterns into normal or attack with a recognition rate of 99% and a false positive rate of 2.25%.

B. New combination: They created a new combination by adding a new layer. The new layer can be a layer from another combination. They postulate that, if this layer is chosen to be the layer responsible for resolving the largest number of neurons, then that can help the other combination.

The proposed enhancement did improve the result. HSOM with PBRM improved the recognition rate from 94.93% to 99%, and gave an acceptable false positive rate, namely 2.25%.

In this work it was shown that SOM is an excellent choice to build IDS.

2.3 Statistical:

Stefan Axelsson and et al. (2004) To counteract the two key deficiencies Low detection rates and a high rate of false alarms, they proposed an interactive detection system based on simple Bayesian statistics combined with a visualisation component. The resulting system was applied to the log of a webserver. The combination proved to be effective. The Bayesian classifier was reasonably effective in learning to differentiate between benign and malicious accesses, and the visualisation component enabled the operator to discern when the intrusion detection system was correct in its output and when it was not, and to take corrective action, re-training the system interactively, until the desired level of performance was reached.

The webserver under study serves a university computer science department. At the time of investigation, the server was running Apache version 1.3.26. It was set to log access requests according to the common log strategy. The log thus consisted of a line based text file with each line representing an single HTTP access request. Cutting out the actual request fields and removing duplicates (i.e. identifying the unique requests that were made) circa 220000 unique requests were identified.

A (prototype) tool named Bayesvis was implemented to apply the principle of interactivity and visualisation to Bayesian intrusion detection. The tool reads messages as text strings and split them up into the substrings that make the tokens. In the first version of the tool URL access requests made up the messages, and they were split according to the URL field separating characters (;/?:@&=+,$) but with little modification the tool could accept any input data that lends itself to being split into messages (perhaps marking sessions) and tokens according to its textual representation.

The 'learning' that a Bayesian system as modelled above does, was encoded in the score of the tokens the IDS use to score the messages. Therefore the scores of the tokens were visualised as their textual representation (black text) on a heatmapped background [23]. Heatmap maped a real number to a colour on the colour wheel, from green via yellow to red that is, the hue of p—in HSV coordinates—was mapped onto the range [180^o, 0^o], fully saturated, and as close to the whitepoint as possible. The total score of the message was visualised in the same manner and also an indicator of whether the user marked this message as benign or malicious.

Iftikhar Ahmad and et al.2009, provided an approach to analyze denial of service attack by using a supervised neural network. The methodology used sampled data from Kddcup99 dataset, an attack database that is a standard for judgment of attack detection tools. The system used multiple layered perceptron architecture and resilient backpropagation for its training and testing. The developed system was then applied to denial of service attacks. Moreover, its performance was also compared to other neural network approaches which resulted in more accuracy and precision in detection rate.

The system was trained on preprocessed data using resilient backpropagation for 1000 epoch. They used full featured packet of DOS attacks from kddcup99 data set [25, 26].

Resilient backpropagation algorithm was used for training of the neural network because it converges very quickly. After the training was completed, the weights of the neural networks were frozen and performance of the neural networks was evaluated. Testing the neural networks involved two steps, which were verification step and recall (or generalization) step. In verification step, neural networks were tested against the data which were used in training. In recall or generalization step, testing was conducted with data which was not used in training. After training, the net only involved computation of the feedforward phase.

In both testing steps performance of the neural networks was evaluated by examining the number of false positives and false negatives that they generated. First they gave packets as input to our system consisting of 11 Back attacks and 5 normal packets. So

the system gave 100 % detection rate and with no any false positive or false negative. It also showed 100% detection rate in case of Land and Neptune attacks.. But in case of Teardown its performance was 79% with 15 % false positives and 6% false negatives rate.

Antonis Papadogiannakis and et al. (2010) presented selective packet discarding, a best effort approach that enables the NIDS to anticipate overload conditions and minimize their impact on attack detection. Instead of letting the packet capturing subsystem randomly drop arriving packets, the NIDS proactively discards packets that are less likely to affect its detection accuracy, and focuses on the traffic at the early stages of each network flow. They presented the design of selective packet discarding and its implementation in Snort NIDS and implemented selective packet discarding in the Snort NIDS as a preprocessor that constantly measures performance aspects of the system in order to detect overload conditions and dynamically adjusts the number of packets that needs to be discarded.

In their first experiment, they explored the impact of imposing a limit in the number of packets of each flow that were going to be processed on Snort's processing throughput and detection accuracy. After that they modified their preprocessor to discard the packets of each flow after a certain flow size limit has been reached. Snort was ran using different flow cutoff values using the augmented network trace.

For 500 Mbit/s traffic, the modified Snort reports 2234 out of the 2252 alerts (99.2%), which was an improvement of 20% over unmodified Snort. The percentage of triggered alerts remains almost constant as the traffic speed increased, falling slightly to 96.3% for 900 Mbit/s traffic, missing just 84 events. They also observed that for all traffic speeds, the modified Snort detected all the 276 real attacks that were manually inserted, suggesting that selective packet discarding indeed tends to improve the detection accuracy of real attacks.

3 COMPARATIVE STUDY

Sr. No.	Author	Proposed Technique	Parameters Considered	Results/Findings
	[1]	proposed a collaborative IDS for MANET using Bayesian method	popular network simulator tool NS2	detection rate= 94.54 %
	[2]	proposed a method with a scalable . solutions for detecting network based anomalies	Support Vector Machines (SVM) plus DGSOT(dynamically growing self organizing tree algorithm)	accuracy found =23% FP =100% (False +ve rate) FN =76% (False –ve rate)
	[3]	introduced a three-tier architecture of intrusion detection system	They used one against one multi-SSVMs	Detection performance=94.71% False alarm =3.8%
	[4]	proposed an intrusion detection . algorithm based on the AdaBoost algorithm	Discrete AdaBoost algorithm	false alarm =.31-1.79% detection rate 90.04%-90.88%
	[5]	proposed an algorithm to use the known signature to find the signature of the related attack quickly	They used 9 different databases from 10 Mbytes to 90 Mbytes	minimum support rate 0.6-0.9 processing time =50 sec(Result obtained for 10 Mb)
	[6]	They proposed Generalized Regression Nueral Network (GRNN) paradigm	KDD CUP 99 Dataset	Accuracy of app=100%
	[7]	Developed a Framework called STAT	Anomaly detection using data mining	speedup=13.8%
	[8]	They proposed a novel architecture which implements a network-based anomaly using unsupervised learning algorithm	They used Two=tier architecture	Detection rate 66.7% False positive=0.03%
	[9]	Presented intrusion detection system & design architecture of intrusion detection based on self organizing map	application of neural network.	formed states were Intrusion-Intrusion

	[10]	developing behavioral models of known attacks to help security Experts.	KDD '99 data set.	By using KDD 10% data set accuracy of attacks perl=100% smurf=99.99% back=88.24% nmap=48.48%
	[11]	presented (ADAPTIVE) automatically tunning IDS	KDD CUP 99 INTRUSION detection dataset	while increasing overall accuracy by by 1.78% ADAT Reduced TMC (total misclassification cost)by 6.76%
	[12]	presented a tools for network anomaly detection and network intelligence i.e. ULISSE	uses a combination of clustering of packets payloads and correlation of anomaliesin the packet stream	Detection Rate=66.7% & FP 0.03%
	[13]	Develop their own Packet sniffer	Dataset contains both packets with intrusion and without intrusion DARPA dataset	The packets were passed through the SOM,results were in the form of patterns.
	[14]	Built a intrusion detection system using Kohonen maps	Performance-Based Ranking Method (PBRM)	For HSOM With PBRM recognition rate =99% False positive rate=2.25% For new combination recognition rate =94.93 to 99% False positive rate=2.25%
	[15]	develop intrusion detection system based on simple Bayesian statistics combined with a visualization component	Web Server	Heatmap a real number of colour on the colour wheel, from green via yellow to red.
	[16]	provide a approach to analyze denial of service attack by using a supervised neural network.	sampled data from KDDCUP 99 data set	detection rate=100% with no any positive or false negative. Land and Nepune attacks:- detection rate =100% Teardown performance:- detection rate =79% false positive rate=15% false negative rate=6%
	[17]	develop selective packet discarding	snort NIDS as a preprocessor	for 500 mbit/s traffic Snort reports 2234 out of the 2252(99.2%)

4 REFERENCES

[1] A. H. M. Rezaul Karim,R, M. A. P. Rajatheva,Kazi M. Ahmed, An Efficient Collaborative Intrusion Detection System for MANET Using Bayesian Approach,pp.187-190,2006.

[2] Latifur Khan · Mamoun Awad · Bhavani Thuraisingham, A New Intrusion Detection System Using Support Vector Machines And Hierarchical Clustering, The VLDB Journal 16,pp. 507 – 521,2007.

[3] Tsong Song Hwang ,Tsung-Ju Lee,Yuh-Jye Lee, A Three-tier IDS via Data Mining Approach, *MineNet'07*, June 12, 2007.

[4] Y.-J. Lee and O. L. Mangasarian. SSVM: A smooth support vector machine. *Computational Optimizationand Applications*, 20:5–22, 2001.

[5] Weiming Hu, ,Steve Maybank, AdaBoost-Based Algorithm for Network Intrusion Detection**,** IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS—PART B: CYBERNETICS, VOL. 38, NO. 2, APRIL 2008 ,PP.577-583

[6] Hu Zhengbing, Li Zhitang,Wu Junq, A Novel Network Intrusion Detection System(NIDS) Based on Signatures Search of Data Mining, *e-Forensics 2008*, January 21-23, 2008, ICST 978-963-9799-19-6.

[7] Amit Kumar Choudhary, Akhilesh Swarup, Neural Network Approach for Intrusion Detection, ICIS 2009, November 24-26, 2009 Seoul, Korea ACM 978-1-60558-710-3.

[8] Giovanni Vigna Fredrik Valeur Richard A. Kemmerer, Designing and Implementing a Family of IntrusionDetection Systems, *ESEC/FSE'03*, September 1–5, 2003, Helsinki, Finland. ACM 1-58113-743-5/03/0009

[9] Stefano Zanero,Sergio M. Savaresi, Unsupervised learning techniques for an intrusion detection system, *SAC'04* March 1417, Nicosia, Cyprus, ACM 1581138121/03/04.

[10] Liberios VOKOROKOS, Anton BALÁŽ, Martin CHOVANEC, Intrusion Detection System Using Self Organising Map,Acta Electrotechnica et Informatica No. 1, Vol. 6, 2006 ,pp.1-6

[11] H. Günes Kayacık, A. Nur Zincir-Heywood, Using Self-Organizing Maps to Build an Attack Map for Forensic Analysis, PST 2006, Oct 30-Nov 1, 2006, Markham, Ontario, Canada, ACM 1-59593-604-1/06/00010.

[12] Zhenwei Yu, Jeffrey J. P. Tsai, An Automatically Tuning Intrusion Detection System, IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS—PART B: CYBERNETICS, VOL. 37, NO. 2, APRIL 2007,pp. 373-384.

[13] Stefano Zanero, ULISSE, a Network Intrusion Detection System, CSIIRW '08 May 12-14, Oak Ridge, Tennessee, USA ACM 978-1-60558-098-2

[14] R. Lippmann, J. W. Haines, D. J. Fried, J. Korba,and K. Das. Analysis and results of the 1999 DARPAo_-line intrusion detection evaluation. In Proceedingsof the Third International Workshop on Recent Advances in Intrusion Detection, pages 162{182,London, UK, 2000. Springer-Verlag.

[15] K. Wang and S. J. Stolfo. Anomalous payload-basednetwork intrusion detection. In RAID Symposium,September 2004.

[16] V. K. Pachghare, Parag Kulkarn, Deven M. Nikam, Intrusion Detection System Using Self Organizing Maps, 978-1-4244-4711-4/09/2009 IEEE.

[17] McHugh, J.: Testing intrusion detection systems: a critique ofthe1998 and 1999 DARPA intrusion detection system evaluationsas performed by lincoln laboratory. ACM Trans. on Informationand System Security 3 (2000) 262-294.

[18] Lane, T., and Brodley, C. E. 1999. Temporal sequence learning and data reduction for anomaly detection. ACM Transactions on Information and System Security 2(3):295-331.

[19] Mansour M. Alsulaiman, Aasem N. Alyahya, Raed A. Alkharboush, Nasser S. Alghafis, Intrusion Detection System using Self-Organizing Maps, 2009 Third International Conference on Network and System Security, 978-0-7695-3838-9/09 ,DOI 10.1109/NSS.2009.62

[20] http://www.securityfocus.com/infocus/1520 - An introduction to IDS,(last checked 15/July/2009)

[21] Srinivas M., Andrew H., "Features Selection for Intrusion detection using Neural Networks and Support Vector Machines",Transportation Research Board, winter 2003.

[22] Stefan Axelsson, Combining a Bayesian Classifier with Visualisation: Understanding the IDS, *VizSEC/DMSEC'04*, October 29, 2004, Washington, DC, USA., ACM 1581139748/04/0010

[23] E. R. Tufte. The Visual Display of Quantitative Information. Graphics Press, second edition, May 2001. ISBN 0–96–139214–2.

[24] Iftikhar Ahmad, Azween B Abdullah, Abdullah S Alghamdi, Application of Artificial Neural Network in Detection of DOS Attacks, *SIN'09*, October 6–10, 2009, North Cyprus, Turkey. ACM 978-1-60558-412-6/09/10.

[25] Iftikhar Ahmad, M.A Ansari, Sajjad Mohsin. "Performance Comparison between Backpropagation Algorithms Applied to Intrusion Detection in Computer Network Systems" in the Book RECENT ADVANCES in SYSTEMS, COMMUNICATIONS & COMPUTERS, Included in ISI/SCI Web of Science and Web of Knowledge & as ACM guide,2008, pp 47-52.

[26] Iftikhar Ahmad, Sami Ullah Swati, Sajjad Mohsin. "Intrusion Detection Mechanism by Resilient Back Propagation (RPROP)" EUROPEAN JOURNAL OF SCIENTIFICRESEARCH, Volume 17, No. 4 August 2007,pp 523-530.

[27] Antonis Papadogiannakis, Michalis Polychronakis, Evangelos P. Markatos, Improving the Accuracy of Network Intrusion Detection Systems Under Load Using Selective Packet Discarding, *EUROSEC* '10, Paris, France , 2010 ACM 978-1-4503-0059-9/10/04.